LIFTS OF PROJECTIVE CONGRUENCE GROUPS

IAN KIMING, MATTHIAS SCHÜTT, HELENA A. VERRILL

Abstract. We show that noncongruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ projectively equivalent to congruence subgroups are ubiquitous. More precisely, they always exist if the congruence subgroup in question is a principal congruence subgroup $\Gamma(N)$ of level $N > 2$, and they exist in many cases also for $\Gamma_0(N)$.

The motivation for asking this question is related to modular forms: projectively equivalent groups have the same spaces of cusp forms for all even weights whereas the spaces of cusp forms of odd weights are distinct in general. We make some initial observations on this phenomenon for weight 3 via geometric considerations of the attached elliptic modular surfaces.

We also develop algorithms that construct all subgroups projectively equivalent to a given congruence subgroup and decide which of them are congruence. A crucial tool in this is the generalized level concept of Wohlfahrt.

1. Introduction

Suppose that Γ_1 and Γ_2 are subgroups of finite index of $\mathrm{SL}_2(\mathbb{Z})$ that are projectively equivalent, i.e., have the same image in $\mathrm{PSL}_2(\mathbb{Z})$. Thus $\langle \Gamma_1, -1\rangle = \langle \Gamma_2, -1\rangle$, and so the space of modular forms of given even weight is the same for the two groups Γ_i. But the spaces of forms of odd weights will in general be different for the two groups (see Section 5 and 8 for concrete examples and results).

The motivations behind the present paper are twofold: first the question whether such a situation can occur with Γ_1 a congruence subgroup but Γ_2 a noncongruence subgroup; and secondly, in such cases to study the attached spaces of cusp forms of odd weights further.

In the present paper we focus primarily on the first question and find that the answer is a resounding 'yes'. More precisely, we give a complete answer to the question in case one of the groups is a principal congruence subgroup $\Gamma(N)$, as well as a partial answer for $\Gamma_0(N)$.

We employ the following terminology: For a subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ denote by $\overline{\Gamma}$ the image of Γ in $\mathrm{PSL}_2(\mathbb{Z})$. By a *lift* of $\overline{\Gamma}$ we mean a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ that projects to $\overline{\Gamma}$ in $\mathrm{PSL}_2(\mathbb{Z})$. A lift is called a *congruence lift* if it is a congruence subgroup.

As usual, if Γ is a congruence subgroup then by the *level* of Γ we understand the least M such that $\Gamma(M) \subset \Gamma$.

Our main results are as follows.

Theorem 1. *Let $N \in \mathbb{N}$ and $\Gamma(N)$ the principal congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ with projective image $\overline{\Gamma(N)} \leq \mathrm{PSL}_2(\mathbb{Z})$.*

2000 *Mathematics Subject Classification.* 11F06; 11F11, 11F32, 11F80, 11G40, 14G10, 14G35, 14J27, 20H05.

(1) *The number* $n(N)$ *of congruence lifts of* $\overline{\Gamma(N)}$ *is exactly*

$$n(N) = \begin{cases} 1 & \text{if } N = 1, \\ 3 & \text{if } N > 1 \text{ is odd}, \\ 5 & \text{if } N = 2, \\ 9 & \text{if } N > 2 \text{ is even}. \end{cases}$$

(2) *If* $N > 2$, *then* $\overline{\Gamma(N)}$ *has noncongruence lifts.*

Theorem 2. *Let* p *be a prime number and let* $N \in \mathbb{N}$.
(i) If $4 \nmid N$ *and all odd prime divisors of* N *are congruent to* 1 *modulo* 4, *then all lifts of* $\overline{\Gamma_0(N)}$ *are congruence.*
(ii) If $p \equiv 3 \ (4)$ *and* $N = p^r$ *for* $r \in \mathbb{N}$, *then there are precisely* 3 *congruence lifts of* $\overline{\Gamma_0(N)}$, *namely* $\Gamma_0(N)$, *the subgroup of* $\Gamma_0(N)$ *consisting of those elements whose diagonal entries are squares modulo* p *and one further subgroup (see Section 7).*
(iii) If N *is divisible by* $6, 9, 16, 20$ *or by a prime* $p > 3$ *congruent to* 3 *modulo* 4, *then the groups* $\overline{\Gamma_0(N)}$ *and* $\overline{\Gamma_1(N)}$ *have noncongruence lifts.*

We will give a detailed discussion of the group $\overline{\Gamma_0(N)}$ for $N = 4, 6, 8, 16, 20$ in section 5. It is shown that all lifts of $\overline{\Gamma_0(N)}$ are congruence if $N = 4, 8$, but that there are noncongruence lifts when $N = 6, 16, 20$.

Thus, as far as the question of existence of noncongruence lifts of the group $\overline{\Gamma_0(N)}$ is concerned, Theorem 2 leaves undecided only the cases where N is $3, 4$ or 8 times an odd number whose prime divisors are all $\equiv 1 \ (4)$.

A crucial tool is a variant of a result of Wohlfahrt [25]. The difference between [25, Theorem 2] and the following proposition is that Wohlfahrt deals with subgroups of $\mathrm{PSL}_2(\mathbb{Z})$ rather than $\mathrm{SL}_2(\mathbb{Z})$. It was a minor surprise to us that his result did not just carry over literally, but that the level N in the conclusion had to be replaced by $2N$. The notion of 'general level' of a subgroup of finite index in $\mathrm{SL}_2(\mathbb{Z})$ (or $\mathrm{PSL}_2(\mathbb{Z})$) will be recalled in section 3.

Proposition 3. *Let* Γ *be a subgroup of finite index in* $\mathrm{SL}_2(\mathbb{Z})$ *of general level* N.
If Γ *is congruence, then* $\Gamma(2N) \leq \Gamma$, *and so* Γ *has level* N *or* $2N$.

The paper is organized as follows: in the first four sections, we establish the techniques that we will use to prove our main results. First we elaborate in generality on lifts of subgroups from $\mathrm{PSL}_2(\mathbb{Z})$ to $\mathrm{SL}_2(\mathbb{Z})$. Then we recall Wohlfahrt's generalized level concept and adjust it to our situation (Proposition 6). In section 4, we derive an algorithm that determines all lifts of a given subgroup of $\mathrm{PSL}_2(\mathbb{Z})$ and decides which of the lifts are congruence (Proposition 10). This algorithm enables us to investigate some examples in detail in section 5.

Sections 6 and 7 continue to give the proofs of Theorems 1 and 2. Next to the level concept and the examples, there is a crucial contribution by information on possible representations of the groups $\overline{\Gamma(N)}$ and $\overline{\Gamma_0(p)}$ (p prime), due to Frasch [6] and Rademacher [19].

The paper concludes with additional observations: first, in section 8, we notice that projective equivalence of subgroups of finite index in $\mathrm{SL}_2(\mathbb{Z})$ not containing -1 is in fact equivalent to the condition that for infinitely many k the groups have the same modular forms of weight k.

Secondly, in section 9 we draw some consequences of our main results for the groups generated by squares of elements in congruence subgroups. We establish results when these groups are again congruence subgroups.

Finally, in section 10 we note some observations on spaces of cusp forms of weight 3 for different lifts. Our arguments are geometric in nature, based on the elliptic modular surfaces attached to the lifts.

2. Preliminaries on lifts

We shall first prove a simple but basic lifting lemma.

Lemma 4. *Consider a subgroup $\overline{\Gamma}$ of $\mathrm{PSL}_2(\mathbb{Z})$ of finite index. Suppose that we are given a presentation of $\overline{\Gamma}$ in terms of generators $\bar{g}_1, \dots \bar{g}_s$ and relations $\bar{R}_1 = 1, \dots, \bar{R}_t = 1$. The relations $\bar{R}_j$ have form:*

$$\bar{R}_j = \prod_{k=1}^{m_j} \bar{h}_{j,k}$$

with each $\bar{h}_{j,k} \in \{\bar{g}_1, \dots \bar{g}_s\}$.

For $i = 1, \dots, s$ and $j = 1, \dots, t$ define the non-negative integer $\sigma_{i,j}$ to be the number of occurrences of $\bar{g}_i$ in the relation $\bar{R}_j$, i.e., the number of $k \in \{1, \dots, m_j\}$ such that $\bar{h}_{j,k} = \bar{g}_i$.

(i). The group $\overline{\Gamma}$ has a lift Γ in $\mathrm{SL}_2(\mathbb{Z})$ such that $-1 \notin \Gamma$ if and only if the $\bar{g}_i$ have lifts $g_i \in \mathrm{SL}_2(\mathbb{Z})$ such that:

$$R_j = 1$$

where for each $j = 1, \dots, t$ the element R_j is defined as the product $\prod_{k=1}^{m_j} h_{j,k}$ where $h_{j,k} := g_i$ if $\bar{h}_{j,k} = \bar{g}_i$.

(ii). Suppose that $\overline{\Gamma}$ has a lift Γ in $\mathrm{SL}_2(\mathbb{Z})$ such that $-1 \notin \Gamma$, given by generators $g_1, \dots g_s$ as in (i).

Then the lifts of $\overline{\Gamma}$ not containing -1 are parametrized by solutions

$$(x_1, \dots, x_s) \in \mathbb{F}_2^s$$

to the linear system of equations

$$(x_1, \dots, x_s)((\sigma_{i,j} \bmod 2))_{i,j} = (0, \dots, 0)$$

over $\mathbb{F}_2$. Here, a given solution $X = (x_1, \dots, x_s)$ corresponds to the subgroup Γ_X of $\mathrm{SL}_2(\mathbb{Z})$ generated by:

$$\{g_i \mid \ x_i = 0\} \cup \{-g_i \mid \ x_i = 1\} \ .$$

Proof. Let α be the canonical homomorphism from $\mathrm{SL}_2(\mathbb{Z})$ onto $\mathrm{PSL}_2(\mathbb{Z})$.

We start by proving *(i)*. The necessity of the condition is clear: Suppose that $\overline{\Gamma}$ has a lift Γ not containing -1. Let $g_i \in \Gamma$ be lifts of the $\bar{g}_i$. The products R_j defined in the proposition then all map to 1 in $\overline{\Gamma}$ under α, and hence $R_j = \pm 1$ for all j. However, the R_j are also elements of Γ, so we must have $R_j = 1$ for all j.

Conversely, suppose that there are lifts g_i such that $R_j = 1$ for $j = 1, \dots, t$. Then let Γ be the subgroup of $\mathrm{SL}_2(\mathbb{Z})$ generated by the g_i.

Since we have the relations $R_j = 1$ among these generators, Γ must be – as an abstract group – a quotient of $\overline{\Gamma}$. Let $\beta : \ \overline{\Gamma} \to \Gamma$ be the corresponding homomorphism. It is given by $\beta(\bar{g}_i) = g_i$.

On the other hand, Γ also surjects to $\overline{\Gamma}$ via α. We have $\alpha(g_i) = \bar{g}_i$.

Now, $(\alpha \circ \beta)(\bar{g}_i) = \bar{g}_i$ for each i and this shows that $\alpha \circ \beta = \mathrm{id}$. Since β is a surjection onto Γ, we conclude that α is injective on Γ. Thus, $-1 \notin \Gamma$.

For the proof of part *(ii)* we first note that it is clear from the above that any lift of $\overline{\Gamma}$ has shape Γ_X for some solution X to the stated system of equations over $\mathbb{F}_2$, and that the group Γ_X is in fact a lift of $\overline{\Gamma}$ for any such solution X. To finish the proof, note that any such Γ_X does not contain -1; this follows because $-1 \notin \Gamma$. For the same reason, we also see that the subgroups corresponding to two distinct solutions X are in fact distinct subgroups. □

We will also need the following observation concerning subgroups of projective groups with noncongruence lifts.

Lemma 5. *Let $\overline{\Gamma}$ be a subgroup of $\mathrm{PSL}_2(\mathbb{Z})$ with a noncongruence lift to $\mathrm{SL}_2(\mathbb{Z})$. Then any subgroup $\overline{G} \leq \overline{\Gamma}$ has a noncongruence lift.*

Proof. Let Γ denote a noncongruence lift of $\overline{\Gamma}$. Define G as the pre-image of $\overline{G}$ under the projection $\Gamma \to \overline{\Gamma}$. By construction, G is a lift of $\overline{G}$ to $\mathrm{SL}_2(\mathbb{Z})$. As a subgroup of the noncongruence subgroup Γ, G cannot be congruence. □

3. Level concept

In this section, we will derive the following restrictions on the level of congruence lifts:

Proposition 6. *Let $N \in \mathbb{N}$ and let $\overline{\Gamma}$ be a subgroup of $\mathrm{PSL}_2(\mathbb{Z})$ with*

$$\overline{\Gamma(N)} \leq \overline{\Gamma} \leq \overline{\Gamma_0(N)} \ .$$

Then any congruence lift of $\overline{\Gamma}$ has level N or $2N$.

In section 5, we will show by means of an example that the proposition cannot be improved: both possibilities N and $2N$ for the level do in fact occur.

To prepare the proof of Proposition 6 we will first recall the generalized notion of level for arbitrary subgroups of finite index in $\mathrm{SL}_2(\mathbb{Z})$, as introduced by Wohlfahrt, cf. [25].

Let Γ be a subgroup of finite index in $\mathrm{SL}_2(\mathbb{Z})$. The general level N of Γ is defined as the least common multiple of the cusp widths. Recall the width of a cusp c of Γ is the least possible $n \in \mathbb{N}$ such that $\pm g T^n g^{-1} \in \Gamma$ where $g \in \mathrm{SL}_2(\mathbb{Z})$ is such that $g\infty = c$, and where T here as well as throughout the paper denotes the usual translation matrix

$$T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Notice that the general level of Γ only depends on $\overline{\Gamma}$. Thus, the general level of any lift of $\overline{\Gamma}(N)$ is N. It is easy to see that if Γ_1 and Γ_2 are two subgroups of finite index in $\mathrm{SL}_2(\mathbb{Z})$, and if $\Gamma_2 \leq \Gamma_1$, then the general level of Γ_1 is a divisor of the general level of Γ_2.

Lemma 7. *Let Γ be a subgroup of finite index in $\mathrm{SL}_2(\mathbb{Z})$. Let N denote the general level of Γ.*

(a). If $\nu \in \mathbb{N}$ is such that $\Gamma(\nu) \leq \Gamma$, then $N \mid \nu$.

(b). Let $N \mid \nu$. Then for any $g \in \mathrm{SL}_2(\mathbb{Z})$, we have $g T^{2\nu} g^{-1} \in \Gamma$.

Proof. (a) By the inclusion $\Gamma(\nu) \leq \Gamma$, the width with respect to Γ of any cusp divides the width with respect to $\Gamma(\nu)$ – which is ν. The claim follows.

(b) Suppose that $N \mid \nu$ and consider any $g \in \mathrm{SL}_2(\mathbb{Z})$. The stabilizer in $\overline{\Gamma}$ of the cusp $g^{-1}\infty$ is $\{\bar{A}^m \mid \ m \in \mathbb{Z}\}$ for a certain matrix $A \in \Gamma$.

Then $g^{-1}Ag$ stabilizes ∞, and by definition of the width b of the cusp $g^{-1}\infty$, we have $g^{-1}Ag = \pm T^b$. By definition of the general level N we have $b \mid N$, hence $b \mid \nu$, and so $\pm gT^\nu g^{-1} = A^{\nu/b} \in \Gamma$. Thus $gT^{2\nu}g^{-1} \in \Gamma$ as desired. □

Let us recall the statement of Proposition 3. The proposition is a slight variant of a result of Wohlfahrt, cf. Theorem 2 of [25] and the succeeding remark.

Proposition. *Let Γ be a subgroup of finite index in $\mathrm{SL}_2(\mathbb{Z})$ of general level N.*

If Γ is congruence, then $\Gamma(2N) \leq \Gamma$, and so Γ has level N or $2N$.

Proof. Suppose that $\nu \in \mathbb{N}$ is such that $\Gamma(\nu) \leq \Gamma$ and let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(2N)$ be arbitrary. We must show that $A \in \Gamma$. Note that it will be enough to show $BAC \in \Gamma$ with matrices $B, C \in \Gamma \cap \Gamma(2N)$, so we can modify A in this way whenever convenient.

We now mimic some computations by Wohlfahrt, cf. [25], proof of Theorem 2 (and in the process also correct a small typo in his argument).

First we claim that we can modify A in the above manner so as to obtain $(d, \nu) = 1$. If $d = \pm 1$ this is already the case, so assume $d \neq \pm 1$. Then $c \neq 0$, but $(c, d) = 1$. Since $A \in \Gamma(2N)$ we have $(d, 2N) = 1$ so that $(d, 2Nc) = 1$. As now $2Nc \neq 0$, we deduce by Dirichlet's theorem on primes in arithmetic progressions that there is $m \in \mathbb{N}$ such that $d + m \cdot 2Nc$ is a prime larger than ν. In particular, this implies $(d + 2Nmc, \nu) = 1$. By Lemma 7 *(b)* we have $T^{2N} \in \Gamma \cap \Gamma(2N)$, and so we may replace A by AT^{2Nm} and thus assume that $(d, \nu) = 1$ (and still $A \in \Gamma(2N)$).

Since now $(d, \nu) = 1$ and $N \mid \nu$ by Lemma 7 *(a)*, we have $(Nd, \nu) = N$. Consequently, $(2Nd, \nu)$ is a divisor of $2N$ which in turn divides b as $A \in \Gamma(2N)$. Hence the congruence $b + n \cdot 2Nd \equiv 0 \ (\nu)$ is solvable for n. Replacing A by $T^{2Nn}A$ does not change d, but changes b to $b + 2Nnd$. So we may additionally assume $b \equiv 0 \ (\nu)$.

Now, again by Lemma 7 *(b)* the matrix

$$\begin{pmatrix} 1 & 0 \\ 2Nm & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} T^{-2Nm} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

is in $\Gamma \cap \Gamma(2N)$ for any $m \in \mathbb{Z}$. With an argument similar to the above we see that if we multiply A on the left by this matrix for a suitable m, we may assume $c \equiv 0 \ (\nu)$. This multiplication leaves b unchanged, and the condition $(d, \nu) = 1$ is preserved since $b \equiv 0 \ (\nu)$.

We now have $b \equiv c \equiv 0 \ (\nu)$ and $(d, \nu) = 1$. Then necessarily $ad \equiv 1 \ (\nu)$.

Now consider the matrix:

$$M = (T^{1-d})' \underbrace{\begin{pmatrix} a & a-1 \\ 1-a & 2-a \end{pmatrix}}_{L} T^{d-1} = \begin{pmatrix} a & ad-1 \\ 1-ad & d(2-ad) \end{pmatrix} \tag{1}$$

where we have denoted by D' the transpose of D for any matrix D.

We find $A \equiv M \mod \nu$, so that $M^{-1}A \in \Gamma(\nu) \leq \Gamma$. To deduce the claim $A \in \Gamma$, it thus suffices to show that $M \in \Gamma$. By Lemma 7 *(b)*, $(T^{1-d})'$ and T^{d-1} are both

in Γ, since $d \equiv 1 \mod 2N$ and $(T^{1-d})'$ is a conjugate of T^{d-1}. Thus it suffices to verify that $L \in \Gamma$. Here we factor

$$L = T'T^{a-1}T'^{-1} .$$

Since $a \equiv 1\ (2N)$, Lemma 7 *(b)* shows that $L \in \Gamma$. Hence we deduce that $M \in \Gamma$ and therefore $A \in \Gamma$ as claimed.

Finally note that the level of Γ is now seen to be N or $2N$ by Lemma 7 *(a)*. □

Remark 8. *In* [25] *Wohlfahrt defines a congruence subgroup of* $\mathrm{SL}_2(\mathbb{Z})$ *as a subgroup containing* $\langle \pm 1, \Gamma(m)\rangle$ *for some* $m \in \mathbb{N}$. *His Theorem 2 states that if* Γ *is a congruence subgroup, then* $\Gamma \geq \langle \pm 1, \Gamma(N)\rangle$ *with* N *the general level of* Γ. *Wohlfahrt's proof essentially coincides with the above proof of Proposition 3 with '*$2N$ *replaced by* N*'. The difference between these cases lies in the fact that if* $-1 \in \Gamma$, *then the conclusion of part (b) of Lemma 7 can be improved to* $gT^{\nu}g^{-1} \in \Gamma$ *as an inspection of the proof immediately reveals. There was a typo in Wohlfahrt's proof that we alluded to above: the matrix* $\left(\begin{smallmatrix} a & ad-1 \\ 1-ad & d(2-ad) \end{smallmatrix}\right)$ *does not equal*

$$(T^{d-1})' \begin{pmatrix} a & a-1 \\ 1-a & 2-a \end{pmatrix} T^{d-1},$$

but factors correctly as in (1).

Remark 9. *The results in this section are also related to results of Larcher, cf.* [10]. *However, he works with a different notion of 'congruence subgroup', namely* -1 *is always assumed to be in the group in contrast to our situation.*

Proof of Proposition 6. Since all lifts of $\overline{\Gamma}$ have the same general level it will suffice by Proposition 3 to display a lift of general level N.

But $\overline{\Gamma}$ has a lift Γ that sits between $\Gamma(N)$ and $\Gamma_0(N)$. Thus the general level of Γ is a divisor of the general level of $\Gamma(N)$ and is a multiple of the general level of $\Gamma_0(N)$. The claim now follows since $\Gamma(N)$ and $\Gamma_0(N)$ both have general level N: all cusps of $\Gamma(N)$ have width N, and the cusp widths of $\Gamma_0(N)$ are all divisors of N, but the cusp 0 has in fact width N. □

4. Algorithm

In the next section, we will investigate two examples that will be used in the proof of Theorem 2. The basis for those examples are the following proposition and its corollary which we believe to be of independent interest.

Proposition 10. *Suppose that a subgroup* $\overline{\Gamma} \leq \mathrm{PSL}_2(\mathbb{Z})$ *of finite index is given by a Farey symbol, or that there is a method of determining whether an element of* $\mathrm{PSL}_2(\mathbb{Z})$ *is in* $\overline{\Gamma}$.

Then there is an algorithm that determines all lifts of $\overline{\Gamma}$ *to* $\mathrm{SL}_2(\mathbb{Z})$ *and decides which of the lifts are congruence.*

Corollary 11. *There is an algorithm that determines all congruence and noncongruence subgroups of* $\mathrm{SL}_2(\mathbb{Z})$ *that are projectively equivalent to a given congruence subgroup.*

4.1. **Farey symbols.** Our algorithm is based on the use of Farey symbols, described in [8]. We recall the definition, with a slight modification, which is necessary because we work with subgroups of $\mathrm{SL}_2(\mathbb{Z})$, whereas Farey symbols as defined in [8] are associated with subgroups of $\mathrm{PSL}_2(\mathbb{Z})$.

Recall Kulkarni's definition [8] of a Farey symbol:

Definition 12. *A Farey symbol consists of a sequence of cusps (elements of $\mathbb{Q}\cup\{\infty\}$), of length $n+1$ for some positive integer $n\geq 1$, starting and ending with infinity, (the starting term can be considered as $-\infty=\frac{-1}{0}$ and the last term as $+\infty=\frac{1}{0}$) together with a sequence of labels $l_1,l_2,\ldots,l_n$ of length n. The sequence of cusps, $\{-\infty,\frac{a_2}{b_2},\frac{a_3}{b_3},\cdots,\frac{a_{n-1}}{b_{n-1}},\infty\}$ satisfies $a_{i+1}b_i-a_ib_{i+1}=1$ for $i=1,\ldots,n-2$, and $b_1=b_{n-1}=1$. Note that we take $a_1=-1,b_1=0$ and $a_{n+1}=1,b_{n+1}=0$. A label is either a positive integer, or a symbol $\circ$ or $\bullet$. For any integer occurring as a label, there are exactly two labels having this value. Such a symbol is written thus:*

$$\{\ -\infty \overset{l_1}{\frown} \frac{a_2}{b_2} \overset{l_2}{\frown} \frac{a_3}{b_3} \overset{l_3}{\frown} \cdots \overset{l_{n-2}}{\frown} \frac{a_{n-1}}{b_{n-1}} \overset{l_{n-1}}{\frown} \frac{a_n}{b_n} \overset{l_n}{\frown} \infty\ \}$$

4.2. **Signed Farey symbols.** Farey symbols correspond to subgroups of $\mathrm{PSL}_2(\mathbb{Z})$. Since we are working with subgroups of $\mathrm{SL}_2(\mathbb{Z})$ not containing -1, we need a minor modification to Farey symbols.

Definition 13. *A signed Farey symbol is defined exactly as a Farey symbol in Definition 12 above, except that the labels can be any nonzero integers, in pairs, or the symbol $\bullet$. The symbol $\circ$ is not used.*

Following Kulkarni, with a minor modification, the subgroup of $\mathrm{SL}_2(\mathbb{Z})$ corresponding to a signed Farey symbol has generators described as follows:

- For any integer pair of integer labels $l_i=l_j$, with $i<j$, we have a generator

$$g_{ij}=\mathrm{sign}(l_i)\begin{pmatrix} a_jb_i+a_{j+1}b_{i+1} & -(a_{i+1}a_{j+1}+a_ia_j)\\ b_ib_j+b_{i+1}b_{j+1} & -(a_ib_j+a_{i+1}b_{j+1})\end{pmatrix}. \tag{2}$$

  Note that it is important to fix the order $i<j$, since changing the order changes the result from a matrix m to $-m^{-1}$.
- For any label $l_j=\bullet$ we have an order 3 generator

$$g_j=\epsilon_j\begin{pmatrix} a_jb_j+a_jb_{j+1}+a_{j+1}b_{j+1} & -(a_{j+1}^2+a_ja_{j+1}+a_j^2)\\ b_j^2+b_jb_{j+1}+b_{j+1}^2 & -(a_jb_j+a_{j+1}b_j+a_{j+1}b_{j+1})\end{pmatrix} \tag{3}$$

  where ϵ_j is chosen so that the matrix has order 3 in $\mathrm{SL}_2(\mathbb{Z})$ (rather than 6). The only relations are those stating that generators corresponding to $\bullet$ have order 3.

Note that for the original Farey symbols, there are additional generators corresponding to labels $l_i=\circ$, namely

$$g_i=\begin{pmatrix} a_ib_i+a_{i+1}b_{i+1} & -(a_i^2+a_{i+1}^2)\\ b_i^2+b_{i+1}^2 & -(a_ib_i+a_{i+1}b_{i+1})\end{pmatrix}. \tag{4}$$

and additional relations, saying that this generator has order 4. However, such groups necessarily contain -1, and so there is no need to consider signs.

Proposition 14. *Any subgroup of finite index in $\mathrm{SL}_2(\mathbb{Z})$ not containing -1 can be defined by a signed Farey symbol, i.e., can be generated by the matrices determined by such a symbol.*

Proof. This follows immediately from [8, (5.4)], Lemma 4, and the fact that edges of Farey symbols labeled $\circ$ correspond to matrices in $\mathrm{SL}_2(\mathbb{Z})$ with square -1, and so do not need to be included in this case. □

If a subgroup Γ of finite index in $\mathrm{SL}_2(\mathbb{Z})$ is given by specifying some rule for determining whether or not an element of $\mathrm{SL}_2(\mathbb{Z})$ is in the group, then the Farey Symbol for Γ is determind as described by [2], and then signs are determined by checking whether or not each of the above matrices are in Γ. If for any i, j both g_{ij} and $-g_{ij}$ are in Γ, then also -1 is in Γ, and so we do not specify any signs for the group. (Similarly for g_i or g_j.)

4.3. **Proof of Proposition 10.** Suppose $\overline{\Gamma}$ is a subgroup of finite index in $\mathrm{PSL}_2(\mathbb{Z})$. We want to determine all congruence lifts of Γ.

Lemma 4 gives an algorithm to determine all lifts of Γ.

Suppose $\overline{\Gamma}$ can be given by a Farey symbol, as described in the previous section, using the method of Kulkarni [8]. For example, this holds true if we can determine whether an element of $\mathrm{PSL}_2(\mathbb{Z})$ is in $\overline{\Gamma}$.

In [9], Lang, Lim and Tan give an algorithm for determining whether $\overline{\Gamma}$ is a projective congruence subgroup. In the case that $\overline{\Gamma}$ is not a congruence subgroup, then all lifts of Γ are also noncongruence, and no more remains to be done.

Suppose that $\overline{\Gamma}$ is determined to be a congruence subgroup of level N by the algorithm in [9]. The algorithm uses a Farey symbol for $\overline{\Gamma}$, and associated generators $\overline{g}_1, \ldots, \overline{g}_s$, and a set of generators $h_1, \ldots, h_k$ for $\Gamma(M)$, where M is the general level N of $\overline{\Gamma}$, and if possible, determines a word for each h_i in terms of the g_j. The same algorithm can also be used when $M = 2N$.

Note that generators and relations of any principal congruence subgroup $\Gamma(M)$ can be obtained algorithmically by using the method of either [3] or [2] applied to the projective image $\overline{\Gamma(M)}$, followed by a simple check to determine sign choices of lifts of generators, and application of Lemma 4 to determine relations.

Suppose that using this method, and once we have determined that $\bar{h}_i = \prod \bar{h}_{i,j}$ for some $\bar{h}_{i,j} \in \{\bar{g}_1, \ldots, \bar{g}_s\}$, then by checking signs, we have

$$h_i = (-1)^{\epsilon_i} \prod h_{i,j},$$

for $i = 1, \ldots, k$ for some $\epsilon_i \in \{0, 1\}$, where each $h_{i,j} \in \{g_1, \ldots, g_s\}$. Let $\sigma_{i,j}$ be the number of times g_i occurs in this product, modulo 2, i.e.,

$$\sigma_{i,j} = \#\{i \mid h_{i,j} = g_j\} \mod 2. \tag{5}$$

Then a lift of Γ having generators $(-1)^{\delta_i} g_i$ for $i = 1, \ldots s$ contains $\Gamma(M)$ if and only if the vector (δ_i) is a solution to the mod 2 linear system of equations

$$(\sigma_{i,j})(\delta_1, \cdots, \delta_s) = (\epsilon_i). \tag{6}$$

By Proposition 6, we need to test whether this is the case for $M = N$ and $M = 2N$. If $\Gamma(N)$ is contained in Γ, it is congruence of level N. If $\Gamma(N)$ is not contained in Γ, but $\Gamma(2N)$ is, then Γ is congruence of level $2N$. Otherwise Γ is not a congruence subgroup. □

Remark 15. *In practice, there will be many generators of* $\Gamma(M)$. *Let* $V_{\Gamma,M}$ *be the space corresponding to writing generators for* $\Gamma(M)$ *as words in terms of the generators for* Γ. *So* $V_{\Gamma,M}$ *is spanned by the vectors in* $\mathbb{F}_2^s$,

$$v_i = (\sigma_{i,1}, \ldots, \sigma_{i,s}) \tag{7}$$

for $i = 1, \ldots, k$, where $\sigma_{i,j}$ are as in (5). We only need take a set of v_i spanning this space in the system (6).

The signs simplify when we have a known congruence lift of level M not containing -1, for example, if Γ is already such a group. Notably this happens for $\Gamma_1(N)$, or if we are considering lifts of $\overline{\Gamma} = \overline{\Gamma_0(p)}$ for p prime, we can take the lift Γ consisting of matrices in $\Gamma_0(p)$ with diagonal entries squares modulo p. In this situation, we can take all $\epsilon_i = 0$.

Remark 16. *Suppose that $\overline{\Gamma}$ has index μ in $\mathrm{PSL}_2(\mathbb{Z})$, has ν_2 elliptic points of order 2, and has ν_3 elliptic points of order 3.*

By Euler's formula applied to the tiling of the fundamental domain for $\overline{\Gamma}$ by images of the fundamental domain for $\mathrm{PSL}_2(\mathbb{Z})$ corresponding to a Farey symbol for $\overline{\Gamma}$, the minimal number of generators of $\overline{\Gamma}$ is

$$\delta := \frac{\mu}{6} + 1 + \frac{\nu_2}{2} + \frac{\nu_3}{3} \ .$$

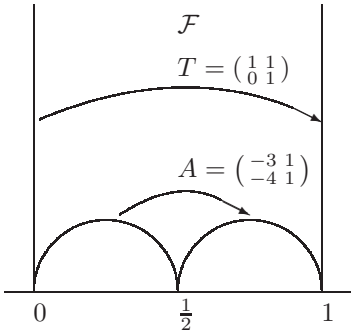
It follows that if $\nu_2 = 0$ then there are $2^{\delta - \nu_3}$ lifts of $\overline{\Gamma}$ not containing -1.

5. Examples

The examples in this section were computed using Pari [18], Magma [1] and GAP [7]. The Magma program has built in functions for determining Farey symbols of congruence subgroups, as described in [8]. A GAP package [5] was also used for computing Farey symbols, and working with subgroups of $\mathrm{PSL}_2(\mathbb{Z})$ given only by their Farey symbol. The algorithm of [9] for determining whether some element of $\mathrm{PSL}_2(\mathbb{Z})$ is in some group given by a Farey symbol was also implemented in GAP.

In some of these examples, we also compute the dimensions of some spaces of cusp forms. The dimensions follow from Shimura's formula which we recall in Section 8. They are given in terms of the number of regular and irregular cusps, ν_∞^+ and ν_∞^- since the subgroups in consideration have no torsion.

Example 17. *Let $\Gamma = \Gamma_1(4)$. A signed Farey symbol with corresponding fundamental domain $\mathcal{F}$ and generators T, A is given in the following diagram:*



$$\overset{+1}{\frown}\ \overset{-2}{\frown}\ \overset{-2}{\frown}\ \overset{+1}{\frown}$$
$$\{\ -\infty \quad \tfrac{0}{1} \quad \tfrac{1}{2} \quad \tfrac{1}{1} \quad \infty\ \}$$

Groups with the same domain $\mathcal{F}$
$G_0 = \langle T, A, -I \rangle = \Gamma_0(4)$
$G_1 = \langle T, A \rangle = \Gamma_1(4)$
$G_2 = \langle T, -A \rangle$
$G_3 = \langle -T, A \rangle$
$G_4 = \langle -T, -A \rangle$

We now apply the algorithm described in Proposition 10. The generators for $\Gamma(4)$ *in terms of* A *and* T *are as follows:*

$$\begin{pmatrix}1&4\\0&1\end{pmatrix} = T^4 \qquad \begin{pmatrix}5&4\\-4&-3\end{pmatrix} = T^{-2}AT$$
$$\begin{pmatrix}1&0\\4&1\end{pmatrix} = A^{-1}T \qquad \begin{pmatrix}5&-4\\4&-3\end{pmatrix} = TA^{-1}$$
$$\begin{pmatrix}-7&12\\4&-7\end{pmatrix} = T^{-2}A^{-1}T^{-1}$$

see the proof of Lemma 32 for more details on the generators of $\Gamma(4)$.

By the algorithm of Proposition 10, we see that level 4 *congruence lifts of* $\overline{\Gamma_1(4)}$ *correspond to solutions of* $\begin{pmatrix}1&1\end{pmatrix}\begin{pmatrix}\delta_1\\\delta_2\end{pmatrix} = \begin{pmatrix}0&0\end{pmatrix}$, *so* $\langle T, A\rangle$ *and* $\langle -T, -A\rangle$ *are congruence subgroups of level* 4.

Using Magma [1] *we compute that* $\Gamma(8)$ *can be generated by* 33 *matrices. Writing these in terms of* A *and* T, *we find that each generator is given as a product of an even number of* A*'s and* T*'s, i.e., the matrix in (6) is the zero matrix, and so the remaining lifts* $\langle -T, A\rangle$ *and* $\langle T, -A\rangle$ *must be congruence subgroups of level* 8.

Thus all four groups $\langle \pm A, \pm T\rangle$ *are congruence subgroups. Being congruence subgroups, they can also be described by congruence conditions by considering the quotients by* $\Gamma(4)$ *or* $\Gamma(8)$.

The table below shows the regularity of the cusps of each lift of $\overline{\Gamma}_0(4)$, *which allows us to compute the dimension of of* $S_3(\Gamma)$ *and* $S_5(\Gamma)$ *for each of these groups. In this table* $S = \left(\begin{smallmatrix}0&1\\-1&0\end{smallmatrix}\right)$ *and* $B = \left(\begin{smallmatrix}1&0\\2&1\end{smallmatrix}\right)$.

cusp	*stabilizer*	*width*	*regular in...?*			
			G_1	G_2	G_3	G_4
∞	T	1	Y	Y	n	n
0	$A^{-1}T = ST^{-4}S^{-1}$	4	Y	n	n	Y
$\frac{1}{2}$	$A = -BT^{-1}B^{-1}$	1	n	Y	n	Y
	$\dim S_3(\Gamma)$		0	0	1	0
	$\dim S_5(\Gamma)$		1	1	2	1
	level as congruence subgroup		4	8	8	4

Example 18. *The group* $\Gamma_1(6)$ *has generators*

$$T = \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right),\ A = \left(\begin{smallmatrix}-5&1\\-6&1\end{smallmatrix}\right),\ B = \left(\begin{smallmatrix}7&-3\\12&-5\end{smallmatrix}\right),$$

corresponding to a Farey symbol

$$\{\ -\infty \overset{+1}{\frown} \tfrac{0}{1} \overset{-2}{\frown} \tfrac{1}{3} \overset{+3}{\frown} \tfrac{1}{2} \overset{+3}{\frown} \tfrac{2}{3} \overset{-2}{\frown} \tfrac{1}{1} \overset{+1}{\frown} \infty\ \}$$

There are no relations between these matrices, so there are 8 *possible subgroups which are lifts of* $\Gamma_1(6)$ *not containing* $-I$. *By Proposition 6 if these are congruence, they have level* 6 *or* 12.

Using Magma [1], *we find that* $\Gamma(6)$ *can be generated by the following 13 matrices. The algorithm of* [9] *expresses these generators in terms of* $g_1 = A, g_2 = B, g_3 = T$. *In the table we also write the corresponding vectors* v_i, *as described in (7) of*

Proposition 10.

$\left(\begin{smallmatrix}-11 & 6\\ -24 & 13\end{smallmatrix}\right)$	$= B^{-2}$	$(0,0,0)$	$\left(\begin{smallmatrix}1 & 0\\ 6 & 1\end{smallmatrix}\right)$	$= A^{-1}T$	$(1,0,1)$
$\left(\begin{smallmatrix}-17 & 6\\ -54 & 19\end{smallmatrix}\right)$	$= (A^{-1}B)^3$	$(1,1,0)$	$\left(\begin{smallmatrix}31 & -12\\ 168 & -65\end{smallmatrix}\right)$	$= (ATA)^{-1}B$	$(0,1,1)$
$\left(\begin{smallmatrix}-29 & 18\\ -108 & 67\end{smallmatrix}\right)$	$= A^{-1}BAB^{-1}$	$(0,0,0)$	$\left(\begin{smallmatrix}-29 & 12\\ -162 & 67\end{smallmatrix}\right)$	$= A^{-1}T^{-2}B$	$(1,1,0)$
$\left(\begin{smallmatrix}19 & -12\\ 84 & -53\end{smallmatrix}\right)$	$= (BA^{-1}BA)^{-1}$	$(0,0,0)$	$\left(\begin{smallmatrix}-71 & 30\\ -258 & 109\end{smallmatrix}\right)$	$= A^{-1}BTB$	$(1,0,1)$
$\left(\begin{smallmatrix}-17 & 12\\ -78 & 55\end{smallmatrix}\right)$	$= A^{-2}BA^{-1}$	$(1,0,0)$	$\left(\begin{smallmatrix}37 & -30\\ 132 & -107\end{smallmatrix}\right)$	$= (ATB^{-1}A)^{-1}$	$(0,1,1)$
$\left(\begin{smallmatrix}-41 & 30\\ -108 & 79\end{smallmatrix}\right)$	$= B^{-1}ABA^{-1}$	$(0,0,0)$	$\left(\begin{smallmatrix}7 & -6\\ 6 & -5\end{smallmatrix}\right)$	$= TA^{-1}$	$(1,0,1)$
$\left(\begin{smallmatrix}-23 & 18\\ -78 & 61\end{smallmatrix}\right)$	$= A^{-1}BA^{-2}$	$(1,0,0)$			

To see if a lift Γ has level 6, we need to check whether all the above matrices are in Γ. We use the algorithm described in Proposition 10. The space $V_{\Gamma_1(6),6}$ spanned by the v_i given in (7) is spanned by $(1,1,0)$ and $(1,0,1)$. The matrices A, B, C generate $\Gamma_1(6)$ which is a lift of $\overline{\Gamma_1(6)}$ not containing -1, so the ϵ_i in (6) are all 0 (as discussed in Remark 15). Thus level 6 congruence lifts of $\overline{\Gamma_0(6)}$ not containing -1 correspond to solutions of

$$\begin{pmatrix}1 & 1 & 0\\ 1 & 0 & 1\end{pmatrix}\begin{pmatrix}\delta_1\\ \delta_2\\ \delta_3\end{pmatrix} = \begin{pmatrix}0 & 0 & 0\end{pmatrix}. \tag{8}$$

The only possible solutions in $\mathbb{F}_2^3$ are $(0,0,0)$ and $(1,1,1)$, and so we find that the only possible congruence level 6 lifts of $\overline{\Gamma_1(6)}$ not containing -1 are $\langle A, B, T\rangle$ and $\langle -A, -B, -T\rangle$.

Using Magma [1], we find that $\overline{\Gamma(12)}$ can be generated by 97 matrices. However, up to parity and rearranging of the letters A, B, T as above, we find that the space $V_{\Gamma_1(6),12}$ spanned by the v_i in (7) is one dimensional, spanned by $(0,1,1)$, corresponding for example to

$$TBA^2 = \left(\begin{smallmatrix}169 & -36\\ 108 & -23\end{smallmatrix}\right).$$

In consequence, the groups $\langle A, B, C\rangle, \langle A, -B, C\rangle, \langle -A, B, -C\rangle, \langle -A, -B, -C\rangle$, all contain $\Gamma(12)$. The remaining lifts are noncongruence subgroups.

The following table shows the data used to compute the dimension of the spaces of weight 3 cusp forms. The last line displays whether the group is a congruence subgroup or not, and if so, its level.

cusp	*stabilizer*	*width*	*regular in …?*			
			$\langle T, A, B\rangle$	$\langle T, -A, B\rangle$	$\langle -T, A, B\rangle$	$\langle -T, -A, B\rangle$
∞	T	1	Y	Y	n	n
0	$AT = (T^{-6})^S$	6	Y	n	n	Y
$\frac{1}{2}$	B	3	Y	Y	Y	Y
$\frac{1}{3}$	$A^{-1}B$	2	Y	n	Y	n
	$\dim S_3(\Gamma)$		0	1	1	1
	level if congruence		6	12	–	–

cusp	*regular in ...?*			
	$\langle T, A, -B\rangle$	$\langle T, -A, -B\rangle$	$\langle -T, A, -B\rangle$	$\langle -T, -A, -B\rangle$
∞	Y	Y	n	n
0	Y	n	n	Y
$\frac{1}{2}$	n	n	n	n
$\frac{1}{3}$	n	Y	n	Y
$\dim S_3(\Gamma)$	1	1	2	1
level if congruence	–	–	12	6

Example 19. $\Gamma_0(8)$ *can be generated by the following matrices:*

$$g_1 = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right),\ g_2 = \left(\begin{smallmatrix} 5 & -1 \\ 16 & -3 \end{smallmatrix}\right),\ g_3 = \left(\begin{smallmatrix} 5 & -2 \\ 8 & -3 \end{smallmatrix}\right).$$

Let $V_8 = V_{\Gamma_0(8),8}$ *be the vector space spanned by the* v_i *of (7), for* $\Gamma(8)$*, and let* $V_{16} = V_{\Gamma_0(8),16}$ *be the space spanned by the* v_i *for* $\Gamma(16)$*. Then* V_8 *is spanned by* $(1, 1, 1)$ *and* $V_{16} = \{0\}$*. So* 4 *of the eight lifts not containing* -1 *are congruence subgroups of level* 8*, and the rest are congruence subgroups of level* 16*.*

Example 20. $\Gamma_0(16)$ *is generated by the following matrices:*

$$g_1 = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right),\ g_2 = \left(\begin{smallmatrix} 5 & -1 \\ 16 & -3 \end{smallmatrix}\right),\ g_3 = \left(\begin{smallmatrix} 25 & -9 \\ 64 & -23 \end{smallmatrix}\right),\ g_4 = \left(\begin{smallmatrix} 9 & -4 \\ 16 & -7 \end{smallmatrix}\right),\ g_5 = \left(\begin{smallmatrix} 13 & -9 \\ 16 & -11 \end{smallmatrix}\right).$$

Let $V_{32} = V_{\Gamma_0(16),32}$ *be the vector space spanned by the* v_i *of (7), for* $\Gamma(32)$*, and let* $V_{16} = V_{\Gamma_0(16),16}$ *be the space spanned by the* v_i *for* $\Gamma(16)$*. Then*

$$V_{16} = \langle (0, 0, 0, 1, 0), (0, 1, 0, 0, 1), (1, 0, 1, 1, 0)\rangle$$

and

$$V_{32} = \langle (0, 1, 0, 0, 1), (1, 0, 1, 0, 0)\rangle$$

So 4 *of the* 32 *lifts not containing* -1 *are congruence subgroups of level* 16*, and* 4 *are congruence subgroups of level* 32*. The remaining* 24 *lifts are noncongruence subgroups.*

Example 21. $\Gamma_0(20)$ *can be generated by the following matrices:*

$$\begin{aligned} g_1 &= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} & g_5 &= \begin{pmatrix} 31 & -9 \\ 100 & -29 \end{pmatrix} \\ g_2 &= \begin{pmatrix} 13 & -2 \\ 20 & -3 \end{pmatrix} & g_6 &= \begin{pmatrix} 17 & -6 \\ 20 & -7 \end{pmatrix} \\ g_3 &= \begin{pmatrix} 31 & -7 \\ 40 & -9 \end{pmatrix} & g_7 &= \begin{pmatrix} 11 & -5 \\ 20 & -9 \end{pmatrix} \\ g_4 &= \begin{pmatrix} 29 & -8 \\ 40 & -11 \end{pmatrix} \end{aligned}$$

Let $V_{40} = V_{\Gamma_0(20),40}$ *be the vector space spanned by the* v_i *of (7), for* $\Gamma(40)$*, and let* $V_{20} = V_{\Gamma_0(20),20}$ *be the space spanned by the* v_i *for* $\Gamma(20)$*. Since* $V_{40} \subset V_{20}$*, we can define a space* W_{20} *with* $V_{20} = V_{40} \oplus W_{20}$*. The following table displays some of the data computed in order to determine the number of congruence lifts of* $\overline{\Gamma_0(20)}$*.*

basis of V_{40}	*basis of* W_{20}	*basis of* $V_{20}^{\perp}$	*basis of* $V_{40}^{\perp}$
$(1, 0, 1, 0, 0, 0, 0)$			$(1, 0, 1, 0, 0, 0, 0)$
$(0, 1, 0, 0, 0, 1, 0)$	$(1, 1, 0, 1, 1, 1, 0)$	$(1, 0, 1, 0, 1, 0, 1)$	$(0, 0, 0, 0, 1, 0, 1)$
$(0, 0, 0, 1, 0, 0, 0)$	$(1, 0, 0, 0, 0, 0, 1)$	$(0, 1, 0, 0, 0, 1, 0)$	$(0, 1, 0, 0, 0, 1, 0)$
$(0, 0, 0, 0, 1, 0, 1)$			

For example, the vector $(0,0,0,0,1,0,1)$ *in* V_{40} *corresponds to*

$$\left(\begin{smallmatrix} -9679 & 2800 \\ -280 & 81 \end{smallmatrix}\right) = g_1^{34} g_7 g_5.$$

From the above data, we see that there are $2^2 = 4$ *congruence lifts of level* 20 *not containing* -1*, and a further* 4 *of level* 40*. The remaining* $2^7 - 8 = 120$ *lifts not containing* -1 *are noncongruence.*

6. Proof of Theorem 1

In this section, we study the principal congruence groups $\overline{\Gamma(N)}$ in $\mathrm{PSL}_2(\mathbb{Z})$ and their lifts to $\mathrm{SL}_2(\mathbb{Z})$. Note that for $N = 1$, i.e. $\mathrm{PSL}_2(\mathbb{Z})$ there is only one lift, the full group $\mathrm{SL}_2(\mathbb{Z})$, since $\pm \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ has square -1.

We refer to $\Gamma(N)$ as the *canonical lift*. For an element $\bar{A} \in \overline{\Gamma(N)}$ we have a unique canonical lift $A_0 \in \Gamma(N)$ if $N > 2$. With respect to the canonical lift A_0, we define the *sign* $\sigma(A)$ of any lift A of $\bar{A}$ as

$$\sigma(A) = \begin{cases} 1, & \text{if } A = A_0, \\ -1, & \text{if } A = -A_0. \end{cases}$$

Let Γ denote any lift of $\overline{\Gamma(N)}$. If Γ is congruence, then $\Gamma(2N) \subset \Gamma$ by Proposition 3. As a consequence, for all $A \in \Gamma$ with $\bar{A} \in \overline{\Gamma(2N)}$, we obtain $\sigma(A) = 1$, i.e. the lift in Γ is fixed as $A = A_0$. Equivalently, for $A, B \in \Gamma$

$$\bar{A} \equiv \bar{B} \mod 2N \implies \sigma(A) = \sigma(B).$$

(We employ the convention that $\bar{A} \equiv \bar{B} \mod 2N$ if and only if $\bar{A}\bar{B}^{-1} \in \overline{\Gamma(2N)}$.)

We now specialize to the situation where N is **odd**. Hence for $A, B \in \Gamma$

$$\bar{A} \equiv \bar{B} \mod 2N \iff A \equiv B \mod 2.$$

Thus we consider the projection from Γ to $\mathrm{SL}_2(\mathbb{F}_2)$ (which is a group homomorphism factoring through the quotient $\overline{\Gamma}$):

$$\begin{array}{ccc} \Gamma & \to & \mathrm{SL}_2(\mathbb{F}_2) \\ A & \mapsto & \tilde{A} \end{array}$$

The congruence property of Γ gives the implication

$$\tilde{A} = \tilde{B} \implies \sigma(A) = \sigma(B). \tag{9}$$

There is one prominent matrix in Γ: the lift of $\bar{T}^N$, which we shall denote by T_N. Apparently its sign can be chosen freely.

Lemma 22. *Let* N *be odd. If* Γ *is congruence and* $-1 \notin \Gamma$*, then the sign of* T_N *fixes the signs of all other elements by (9).*

Proof. Let $A \in \Gamma$. We shall use the fact that $\mathrm{SL}_2(\mathbb{F}_2) \cong S_3$. If $\tilde{A}$ has odd order, then $\tilde{A}^3 = 1$. Hence $\sigma(A) = \sigma(A^3) = 1$. If $\tilde{A}$ has order two, then either $\tilde{A} = \tilde{T}_N$ or $\tilde{A}\tilde{T}_N$ has order three. In each case $\sigma(A) = \sigma(T_N)$. □

Corollary 23. *If* $N > 1$ *is odd, then* $\overline{\Gamma(N)}$ *has exactly three congruence lifts.*

Namely the congruence lifts are $\Gamma(N), \{\pm 1\} \cdot \Gamma(N)$ and the subgroup generated by $-T^N$ and the appropriate lifts of the other generators of $\overline{\Gamma(N)}$ as determined by Lemma 22. By construction, each of these lifts contains $\Gamma(2N)$.

Corollary 24. *If $N > 1$ is odd, then $\overline{\Gamma(N)}$ has noncongruence lifts.*

Since $\overline{\Gamma(N)}$ cannot be generated by a single element, the corollary follows readily. For $N = p$, we obtain explicit numbers from Frasch's work [6]: $\overline{\Gamma(p)}$ is freely generated by $r = 1 + p\,(p^2-1)/12$ elements, so we have three congruence lifts and $2^r - 2$ noncongruence lifts.

We now turn to **even** level N. Here $\Gamma(N)/\Gamma(2N) \cong (\mathbb{Z}/2)^3$ by virtue of the following construction: Let $A \in \Gamma(N)$. Write A uniquely as

$$A = 1 + N \cdot B + 2N \cdot C, \quad B \in M_2(\mathbb{F}_2),\ C \in M_2(\mathbb{Z}).$$

Here $1 = \det(A) = 1 + N\,\mathrm{tr}(B) + 2N\,(\ldots)$. In consequence, B has even trace. This defines a group homomorphism

$$\begin{array}{rcl} \Gamma(N) & \to & M_2(\mathbb{F}_2) \\ A & \mapsto & \hat{A} = B \end{array}$$

with kernel $\Gamma(2N)$ and image the matrices in $M_2(\mathbb{F}_2)$ with zero trace. Hence it identifies the quotient $\Gamma(N)/\Gamma(2N)$ with the image, i.e. abstractly with $(\mathbb{Z}/2)^3$.

First we consider the case $N > 2$. Since $-1 \notin \Gamma(N)$, there are canonical lifts. Hence for any lift Γ of $\overline{\Gamma(N)}$, we obtain a group homomorphism

$$\Gamma \ni A \mapsto \bar{A} \mapsto A_0 \mapsto \hat{A} = \hat{A}_0.$$

As before, if Γ is congruence, then it contains $\Gamma(2N)$ by Proposition 3. Hence we have

$$\hat{A} = \hat{B} \ \Rightarrow\ \bar{A} \equiv \bar{B} \mod 2N \ \Rightarrow\ \sigma(A) = \sigma(B).$$

It follows that the signs of three elements with independent image in $M_2(\mathbb{F}_2)$ determine the congruence lift Γ. Here two signs are given by the elements $T_N, T_N' \in \Gamma$. The third sign is fixed by the lift of

$$\begin{pmatrix} 1+N & -N \\ N & 1-N \end{pmatrix}.$$

As in the case of odd N, the sign restrictions determine all congruence lifts of $\overline{\Gamma(N)}$:

Lemma 25. *Let $N > 2$ be even. Then $\overline{\Gamma(N)}$ has exactly 9 congruence lifts.*

Corollary 26. *If $N > 2$, then $\overline{\Gamma(N)}$ has noncongruence lifts.*

Proof. For odd $N > 1$, this result is Corollary 24. For even $N > 2$, it will follow from Lemma 5, once we verify the claim for $N = 4$. To this end, it suffices to check that $\overline{\Gamma(4)}$ has at least four free generators. In fact, we have seen in Example 17 that $\overline{\Gamma(4)}$ has five free generators. □

To complete the proof of Theorem 1, we are concerned with the remaining case $N = 2$. Here the situation differs since $-1 \in \Gamma(2)$. Nonetheless we can define a non-trivial canonical lift $\Gamma_0 \subsetneq \Gamma(2)$ by requiring

$$a \equiv d \equiv 1 \mod 4$$

for the diagonal entries of any matrix in Γ_0. Then we proceed as before with the only difference that the image of Γ_0 in $M_2(\mathbb{F}_2)$ consists of all matrices with zero diagonal elements. Abstractly, the image is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$. This agrees with the generators of $\Gamma(2)$ being $-1, T^2, (T^2)'$ by [6]. Hence any non-trivial lift

Γ of $\overline{\Gamma(2)}$ is generated by the lifts T_2, T_2'. By the above consideration, for Γ to be congruence we can choose the signs of both generators freely. Hence all five lifts are congruence.

Alternatively, one could deduce this claim from the fact that $\Gamma(2)^2 = \Gamma(4)$ as we will show in section 9.

7. Proof of Theorem 2

Let us first recall some well-known facts about elements of finite order of $\mathrm{SL}_2(\mathbb{Z})$, cf. [21], Propositions 1.12 and 1.18: an element $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ different from ± 1 has finite order if and only if $|a+d| < 2$. An easy computation then shows that -1 is the only element of order 2, whereas the elements of order 4 are precisely the elements of form

$$\begin{pmatrix} a & b \\ c & -a \end{pmatrix}$$

where $a, b, c \in \mathbb{Z}$ with $a^2 + bc = -1$.

Proof of (i). Write $N = 2^s \cdot p_1^{s_1} \cdots p_t^{s_t}$ where $s \leq 1$ and the p_i are distinct primes each congruent to 1 modulo 4.

Thus for each i, the number -1 is a square in $\mathbb{Z}_{p_i}$, i.e. the congruence $x^2 \equiv -1 \ (p_i^r)$ is solvable in $\mathbb{Z}$ for every $r \in \mathbb{N}$. Since $s \leq 1$ the same holds trivially true for the congruence $x^2 \equiv -1 \ (2^s)$. By the Chinese Remainder Theorem we conclude that there is $a \in \mathbb{Z}$ such that $a^2 \equiv -1 \ (N)$.

Consequently there exists an element $\gamma = \left(\begin{smallmatrix} a & b \\ N & -a \end{smallmatrix}\right)$ of order 4 in $\Gamma_0(N)$. If now Γ is a lift of $\overline{\Gamma_0(N)}$ we must have $\gamma \in \Gamma$ or $-\gamma \in \Gamma$. Since the square of both γ and $-\gamma$ is -1, we conclude that Γ contains -1 and hence equals $\Gamma_0(N)$. □

Proof of (ii). Let p be an odd prime, $p \equiv 3 \ (4)$ and $N = p^r$ for some $r \in \mathbb{N}$. Denote by $(\cdot/p)$ the Legendre symbol modulo p. We define the sign homomorphism

$$\begin{array}{rccc} \sigma: & \Gamma_0(N) & \to & \{\pm 1\} \\ & \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \mapsto & \left(\dfrac{a}{p}\right) \end{array}$$

Then $G_1 = \ker(\sigma)$ is a congruence subgroup of $\Gamma_0(N)$, since $\Gamma_1(N) \subset G_1$. The subgroup G_1 consists exactly of those matrices in $\Gamma_0(N)$ whose diagonal entries are squares modulo p (or equivalently modulo N).

Let Γ be a congruence lift of $\overline{\Gamma_0(N)}$. By Proposition 3 we have then $\Gamma(2N) \leq \Gamma$. Note that σ is trivial on $\Gamma(2N)$. Hence σ factors through the quotient $\Gamma/\Gamma(2N)$.

In order to study this quotient, consider the homomorphism

$$\phi: \ \mathrm{SL}_2(\mathbb{Z})/\Gamma(2N) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/2) \times \mathrm{SL}_2(\mathbb{Z}/N)$$

given by $A \mapsto (A \bmod 2, A \bmod N)$; ϕ is an isomorphism: it is clearly injective, and hence surjective by comparison of orders (cf. for instance [14], Theorem 4.2.5, for formulas for indices of the various subgroups in $\mathrm{SL}_2(\mathbb{Z})$). Under this isomorphism, $\Gamma_0(N)$ is mapped to

$$\phi(\Gamma_0(N)) =: G = \mathrm{SL}_2(\mathbb{Z}/2) \times H \leq \mathrm{SL}_2(\mathbb{Z}/2) \times \mathrm{SL}_2(\mathbb{Z}/p)$$

where $H \cong \Gamma_0(N)/\Gamma(N)$: clearly the image is contained in $\mathrm{SL}_2(\mathbb{Z}/2) \times H$ and hence equals this group, again by order considerations:

$$[\Gamma_0(N) : \Gamma(2N)] = 6p^{2r-1}(p-1) = 6 \cdot [\Gamma_0(N) : \Gamma(N)] = \#(\mathrm{SL}_2(\mathbb{Z}/2)) \cdot [\Gamma_0(N) : \Gamma(N)].$$

For $A \in \Gamma_0(N)$, $\sigma(A)$ is determined by the image of A in H. Hence we shall study the structure of H to some extent. In the present situation, H is not cyclic, but close enough to it in the following sense:

Lemma 27. *For any $A \in H$, we have $A^u = \pm 1$ for $u = p^{2r-1}(p-1)/2$.*

Proof. We will use the immediate fact for $A \in \Gamma_0(N)$ with diagonal entries a, d that A^t has diagonal entries a^t, d^t modulo N. Here $N = p^r$ so that $(\mathbb{Z}/N\mathbb{Z})^*$ is cyclic of order $p^{r-1}(p-1)$. Thus for any $A \in \Gamma_0(N)$, $A^{p^{r-1}(p-1)/2}$ has diagonal entries ± 1. But then for any $B \in \Gamma_0(N)$ with diagonal entries ± 1, we have $B^{p^r} = \pm 1$. □

Corollary 28. *For any $A \in \Gamma_0(N)$, we have*

$$\sigma(A) = \begin{cases} 1 & \text{if } A \text{ has odd order in } H; \\ -1 & \text{if } A \text{ has even order in } H. \end{cases}$$

Proof. Since $u = p^{2r-1}(p-1)/2$ is odd, we have $\sigma(A) = \sigma(A^u)$ where $A^u = \pm 1$ in H depending on the parity of the order. The distinction of the two cases follows directly. □

We return to the congruence lift Γ of $\Gamma_0(N)$. Suppose that $-1 \notin \Gamma$. Then, since -1 is not in the kernel of ϕ, we have that $\phi(\Gamma)$ is a subgroup of index 2 of G, and G is generated by $\phi(G)$ and $\phi(-1)$. In particular $\phi(-1) = (1,-1) \notin \phi(G)$.

Proposition 29. *Let $\Gamma \neq G_1, \Gamma_0(N)$ be a congruence lift. Then σ is determined on Γ by the relation*

$$\sigma(A) = -1 \iff A \text{ has order two in } \mathrm{SL}_2(\mathbb{Z}/2).$$

Proof. Since $\Gamma \neq G_1$, there is $B \in \Gamma$ such that $\sigma(B) = -1$. Let $C := B^u$. Then $\sigma(C) = -1$, so that $C = -1$ in H by Lemma 27 and Corollary 28. But then since $(1,-1) \notin \phi(G)$, we deduce that C has order two in $\mathrm{SL}_2(\mathbb{Z}/2)$.

First we let $A \in \Gamma$ have odd order in $\mathrm{SL}_2(\mathbb{Z}/2)$. Then $\phi(A^{3u}) = (1,1)$ since $A^{3u} = \pm 1$ in H, but $(1,-1) \notin \phi(\Gamma)$. Hence $\sigma(A) = \sigma(A^{3u}) = 1$.

Now let $A \in \Gamma$ have order two in $\mathrm{SL}_2(\mathbb{Z}/2)$. In consequence $A \cdot C$ has odd order in $\mathrm{SL}_2(\mathbb{Z}/2)$. By the first alternative, we obtain $1 = \sigma(A \cdot C) = -\sigma(A)$. □

We are now ready to prove the second statement from Theorem 2. Namely the order in $\mathrm{SL}_2(\mathbb{Z}/2)$ does not depend on the lift from $\mathrm{PSL}_2(\mathbb{Z})$ to $\mathrm{SL}_2(\mathbb{Z})$. Hence the sign condition in Proposition 29 determines the lift $\Gamma \neq G_1, \Gamma_0(N)$ uniquely. This lift Γ is in fact congruence as it contains $\Gamma(2N)$ by definition. □

Proof of (iii). We start by utilizing results of Rademacher to treat the prime case $N = p$:

Lemma 30. *If $p \equiv 3\,(4)$ with $p > 3$, then there are noncongruence lifts of $\overline{\Gamma_0(p)}$. More precisely, putting*

$$s := 2\left[\frac{p}{12}\right] + 3$$

the number of noncongruence lifts of $\overline{\Gamma_0(p)}$ is:

$$\begin{cases} 0 & \text{if } p = 3 \\ 2^{s-2} - 2 & \text{if } p \equiv 7 \quad (12) \\ 2^s - 2 & \text{if } p \equiv 11 \quad (12). \end{cases}$$

Proof. By [19, pp. 146–147], we know that if $p > 3$ then the group $\overline{\Gamma_0(p)}$ is generated by

$$s := 2\left[\frac{p}{12}\right] + 3$$

elements and relations as follows. If $p \equiv 11\ (12)$ there are no relations, whereas if $p \equiv 7\ (12)$ there are 2 relations involving two of the generators, call them V_1 and V_2, namely

$$V_1^3 = V_2^3 = 1\ .$$

By Lemma 4 we can determine the number of lifts when $p > 3$: in the cases $p \equiv 11\ (12)$ and $p \equiv 7\ (12)$, there are precisely 2^s resp. 2^{s-2} lifts of $\overline{\Gamma_0(p)}$ not containing -1. By Theorem 2 *(ii)* there are precisely two congruence lifts not containing -1. Thus the formulas for the number of noncongruence lifts follow when $p > 3$. One checks immediately that this number is positive in all cases.

As for the group $\overline{\Gamma_0(3)}$, by [19] it is generated by two elements S and V with the single relation $V^3 = 1$. Hence Lemma 4 implies that the group admits precisely two lifts not containing -1. Both lifts are congruence by Theorem 2 *(ii)*. □

Let N be as in Theorem 2 *(iii)*. We have seen in the section 5, that there are noncongruence lifts of the groups $\overline{\Gamma}_0(6), \overline{\Gamma_0(16)}$ and $\overline{\Gamma_0(16)}$. Using Theorem 2 *(ii)* one can prove the same for $\overline{\Gamma_0(9)}$, since this group has more than one free generator. Thus, by the hypothesis and by Lemma 30, there is a divisor M of N such that $\overline{\Gamma_0(M)}$ has a noncongruence lift. Let now $\overline{G}$ be any of the groups $\overline{\Gamma_0(N)}$ and $\overline{\Gamma_1(N)}$. Then $\overline{G} \leq \overline{\Gamma_0(M)}$, and the claim follows from Lemma 5. □

Theorem 2 leaves essentially three cases unanswered: $3, 4$ or 8 times a product of primes congruent to 1 modulo 4. An analysis of this case requires different techniques that we hope to address elsewhere.

8. Subgroups with the same cusp forms

Suppose that Γ_1 and Γ_2 are subgroups of finite index in $\mathrm{SL}_2(\mathbb{Z})$. Let $S_k(\Gamma_i)$ denote the space of cusp forms of weight k with respect to Γ_i. If the groups contain -1, then $S_k(\Gamma_1) = 0 = S_k(\Gamma_2)$ for all odd k. In particular this holds for infinitely many k.

Now consider the case where the groups do not contain -1. We will show that $S_k(\Gamma_1) = S_k(\Gamma_2)$ holds for infinitely many k only if the groups are projectively equivalent. More precisely:

Proposition 31. *(i). Suppose that G and Γ are subgroups of $\mathrm{SL}_2(\mathbb{Z})$ of finite index and that Γ is a subgroup of G.*

Suppose that we have $\dim S_k(G) = \dim S_k(\Gamma)$ for infinitely many positive integers k, and that either infinitely many of these k are even, or that $-1 \notin \Gamma$.

Then $\overline{G} = \overline{\Gamma}$.

(ii). Let Γ_1 and Γ_2 be subgroups of $\mathrm{SL}_2(\mathbb{Z})$ of finite indices and suppose that -1 is not in $\Gamma_1 \cap \Gamma_2$.

Then $S_k(\Gamma_1) = S_k(\Gamma_2)$ for infinitely many $k \in \mathbb{N}$ if and only if $\overline{\Gamma}_1 = \overline{\Gamma}_2$.

Proof of (i). Let γ denote the genus of the modular curve $\Gamma\backslash\mathcal{H}^*$. Here as usual, $\mathcal{H}^*$ denotes the upper halfplane with the cusps $\mathbb{Q}\cup\{\infty\}$ added. Let $\mu := [\mathrm{PSL}_2(\mathbb{Z}) : \overline{\Gamma}]$, let ν_2 and ν_3 denote the number of inequivalent elliptic points of Γ of orders 2 and

3, respectively, let ν_∞ be the number of inequivalent cusps of Γ, and let ν_∞^+ and ν_∞^- denote the number of inequivalent regular and irregular cusps of Γ, respectively. Thus, $\nu_\infty = \nu_\infty^+ + \nu_\infty^-$.

If k is even and > 2 we have by the dimension formula, cf. [14], Theorem 2.5.2, that

$$\dim S_k(\Gamma) = (k-1)(\gamma-1) + \frac{k-2}{2}\cdot\nu_\infty + \left[\frac{k}{4}\right]\cdot\nu_2 + \left[\frac{k}{3}\right]\cdot\nu_3$$

and also

$$\gamma = 1 + \frac{\mu}{12} - \frac{\nu_2}{4} - \frac{\nu_3}{3} - \frac{\nu_\infty}{2}$$

by the genus formula, cf. [21], Proposition 1.40. Thus,

$$\dim S_k(\Gamma) = \frac{k-1}{12}\cdot\mu - \frac{\nu_\infty}{2} + \left(\left[\frac{k}{4}\right] - \frac{k-1}{4}\right)\cdot\nu_2 + \left(\left[\frac{k}{3}\right] - \frac{k-1}{3}\right)\cdot\nu_3$$

for k even and > 2.

Similarly, if $-1 \notin \Gamma$ and $k \geq 3$ is odd we have the dimension formula [14], Theorem 2.5.3:

$$\dim S_k(\Gamma) = (k-1)(\gamma-1) + \frac{k-2}{2}\cdot\nu_\infty^+ + \frac{k-1}{2}\cdot\nu_\infty^- + \left[\frac{k}{4}\right]\cdot\nu_2 + \left[\frac{k}{3}\right]\cdot\nu_3$$

which combines with the genus formula to:

$$\dim S_k(\Gamma) = \frac{k-1}{12}\cdot\mu - \frac{\nu_\infty^+}{2} + \left(\left[\frac{k}{4}\right] - \frac{k-1}{4}\right)\cdot\nu_2 + \left(\left[\frac{k}{3}\right] - \frac{k-1}{3}\right)\cdot\nu_3$$

where we used $\nu_\infty = \nu_\infty^+ + \nu_\infty^-$.

Now note that we have similar formulas for $\dim S_k(G)$, that for any $a \in \mathbb{N}$ the number $\left[\frac{k}{a}\right] - \frac{k-1}{a}$ stays bounded for $k \to \infty$, and that if we have $-1 \notin \Gamma$ and $\dim S_k(G) = \dim S_k(\Gamma)$ for infinitely many odd k, then necessarily $S_k(G) \neq 0$ for some odd k and thus $-1 \notin G$. Combining our hypothesis with an asymptotic consideration then shows that we necessarily have

$$[\mathrm{PSL}_2(\mathbb{Z}) : \overline{\Gamma}] = \mu = [\mathrm{PSL}_2(\mathbb{Z}) : \overline{G}]$$

and hence $\overline{G} = \overline{\Gamma}$ since $\overline{G} \leq \overline{\Gamma}$.

Proof of (ii). If $\overline{\Gamma}_1 = \overline{\Gamma}_2$, then $S_k(\Gamma_1) = S_k(\Gamma_2)$ for all even $k \in \mathbb{N}$.

Conversely, suppose that $S_k(\Gamma_1) = S_k(\Gamma_2)$ for infinitely many $k \in \mathbb{N}$. Consider the group G generated by Γ_1 and Γ_2. If k is such that $S_k(\Gamma_1) = S_k(\Gamma_2)$, then $S_k(G) = S_k(\Gamma_i)$ for $i = 1, 2$.

By hypothesis, $-1 \notin \Gamma_1$ or $-1 \notin \Gamma_2$, say $-1 \notin \Gamma_1$. Then we obtain $\overline{\Gamma}_1 = \overline{G}$ by *(i)*.

If $-1 \notin \Gamma_2$, then $\overline{\Gamma}_2 = \overline{G}$ by *(i)* as claimed. If $-1 \in \Gamma_2$, then $S_k(\Gamma_2) = 0$ for odd k. On the other hand, as $-1 \notin \Gamma_1$ we have $S_k(\Gamma_1) \neq 0$ for all sufficiently large odd k. Thus, our hypothesis would imply $S_k(G) = S_k(\Gamma_1) = S_k(\Gamma_2)$ for infinitely many even k. Hence $\overline{\Gamma}_2 = \overline{G}$ by *(i)*.

Thus, in any case, $\overline{\Gamma}_1 = \overline{G} = \overline{\Gamma}_2$, as desired. □

9. Squares of congruence subgroups

We note a consequence for the subgroup Γ^2 generated by squares in a given subgroup Γ. From Theorem 1, we can deduce immediately that $\Gamma(N)^2$ is not congruence when $N > 2$: this follows from Lemma 5 since any lift of $\overline{\Gamma}(N)$ necessarily contains $\Gamma(N)^2$ (if Γ is a lift and if $g \in \Gamma(N)$ then Γ contains either g or $-g$, and hence in any case g^2). Thus, if $\Gamma(N)^2$ is congruence, then all lifts of $\overline{\Gamma}(N)$ are congruence.

On the other hand, it is known that $\Gamma(1)^2$ is congruence: in fact, $\Gamma(2) \subset \Gamma(1)^2$ by [15]. (The inclusion $\Gamma(6) \subset \Gamma(1)^2$ was previously proven by J. R. Smith in his 1961 thesis at Michigan State, cf. [16].)

This leaves open the case of $\Gamma(2)^2$ which we can solve with the techniques from section 4.

Lemma 32. $\Gamma(2)^2 = \Gamma(4)$.

Proof. Consider the following Farey symbol for $\Gamma(4)$.

$$\{\ -\infty \overset{+1}{\frown} \tfrac{-2}{1} \overset{-2}{\frown} \tfrac{-3}{2} \overset{+3}{\frown} \tfrac{-1}{1} \overset{+3}{\frown} \tfrac{-1}{2} \overset{+4}{\frown} \tfrac{0}{1} \overset{+4}{\frown} \tfrac{1}{2} \overset{+5}{\frown} \tfrac{1}{1} \overset{+5}{\frown} \tfrac{3}{2} \overset{-2}{\frown} \tfrac{2}{1} \overset{+1}{\frown} \infty\ \}$$

That this is a Farey symbol for $\Gamma(4)$ follows from the fact that all the corresponding generating matrices are in $\Gamma(4)$, and this Farey symbol corresponds to a group with index 24 in $\mathrm{PSL}_2(\mathbb{Z})$, which is equal to $[\mathrm{PSL}_2(\mathbb{Z}) : \overline{\Gamma(4)}]$ using the well known formula.

We can write the generating matrices in terms of squares of elements of $\Gamma(2)$ thus:

$$\begin{aligned}
\left(\begin{smallmatrix} 1 & 4 \\ 0 & 1 \end{smallmatrix}\right) &= \left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right)^2 \\
\left(\begin{smallmatrix} -7 & 12 \\ 4 & -7 \end{smallmatrix}\right) &= \left(\left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right)^2\right)^{-1} \left(\begin{smallmatrix} 5 & -8 \\ 2 & -3 \end{smallmatrix}\right)^2 \\
\left(\begin{smallmatrix} 5 & 4 \\ -4 & -3 \end{smallmatrix}\right) &= \left(\begin{smallmatrix} -3 & -2 \\ 2 & 1 \end{smallmatrix}\right)^2 \\
\left(\begin{smallmatrix} 1 & 0 \\ 4 & 1 \end{smallmatrix}\right) &= \left(\begin{smallmatrix} 1 & 0 \\ 2 & 1 \end{smallmatrix}\right)^2 \\
\left(\begin{smallmatrix} 5 & -4 \\ 4 & -3 \end{smallmatrix}\right) &= \left(\begin{smallmatrix} -3 & 2 \\ -2 & 1 \end{smallmatrix}\right)^2
\end{aligned}$$

This demonstrates that $\Gamma(4) \subseteq \Gamma(2)^2$. On the other hand, we can easily check that the square of any element of $\Gamma(2)$ must be in $\Gamma(4)$ (since if $A - I = 2B$ for some matrices A, B with integer entries, then $A^2 - I = (2B + I)^2 - I = 4B(B + I)$), so $\Gamma(2)^2 \subseteq \Gamma(4)$. Hence the two groups are equal. □

In consequence, we can identify the principal congruence subgroups whose squares are congruence again:

Proposition 33. *$\Gamma(N)^2$ is congruence if and only if $N \leq 2$.*

Along the same lines, we obtain from Theorem 2 *(iii)* with Lemma 5:

Corollary 34. *If N is divisible by $6, 9, 16, 20$ or by a prime $p > 3$ congruent to 3 modulo 4, then $\Gamma_0(N)^2$ and $\Gamma_1(N)^2$ are not congruence.*

For future use in the general case, we also note the following lemma which slightly simplifies the congruence question for squares:

Lemma 35. *If Γ has general level N and Γ^2 is congruence, then Γ^2 has level $2N$.*

Proof. Arguing with the cusps as before, we see that Γ^2 has general level $2N$. Hence if Γ^2 is congruence, then the level divides $4N$ by Proposition 3.

Looking at the proof of Proposition 3, the main difference when working with Γ^2 is that $T^{2N} \in \Gamma^2$ due to the assumption that Γ has general level N. Hence Wohlfahrt's original argument goes through without doubling the level twice, since this was only necessary to ensure that T^{2N} is contained in the group. Thus Γ^2, if it is congruence, has level $2N$. □

Remark 36. *With the generators in the proof of Lemma 32, we can also give a more precise description of the lifts of* $\overline{\Gamma(4)}$*: Any congruence lift of* $\overline{\Gamma(4)}$ *must have level either* 4 *or* 8 *by Proposition 6. With* $V_4 = V_{\Gamma(4),4}$ *and* $V_8 = V_{\Gamma(4),8}$*, as described in Remark 15, in terms of the above set of generators, we have*

$$V_4^\perp = 0, \text{ and } V_8 = \langle (0,0,1,0,1), (1,1,0,1,0) \rangle$$

So there is a unique level 4 *congruence lift of* $\overline{\Gamma(4)}$ *not containing* -1*, namely* $\Gamma(4)$*, and a further* 7 *level* 8 *lifts, in accordance with Lemma 25; the remaining* 24 *lifts are noncongruence.*

10. Elliptic modular surfaces

We conclude this paper with some geometric considerations. Our motivation stems from modular forms. We have seen in section 8 that lifts can only be distinguished on modular forms of odd weight. For weight 3, there is an instructive relation to holomorphic 2-forms on certain complex algebraic surfaces that we shall briefly recall.

Let Γ denote a finite index subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ not containing -1. A construction by Shioda associates Γ with an elliptic modular surface $S(\Gamma)$ over the modular curve $X(\Gamma)$ (uniquely up to $\mathbb{C}$-isomorphism) [22]. For congruence subgroups, this construction simply exhibits the universal modular curve.

Throughout this paper, we have been considering different lifts. In particular, the modular curve $X(\Gamma)$ is the same for all lifts, as it only depends on the image $\bar{\Gamma}$ of Γ in $\mathrm{PSL}_2(\mathbb{Z})$. For shortness, we write $X = X(\Gamma), S = S(\Gamma)$.

Of course, the j-map

$$j : \quad X \to \mathbb{P}^1$$

is also independent of the lift. On the other hand, S is determined by j only up to quadratic twisting. This notion refers to non-isomorphic elliptic curves which become isomorphic over a quadratic extension of the ground field. In terms of an extended Weierstrass form

$$y^2 = x^3 + Ax^2 + Bx + C, \quad A, B, C \in k,$$

quadratic twists are in correspondence with squarefree elements $d \in k$. The twist by d is exhibited by the Weierstrass form

$$y^2 = x^3 + dA^2x + d^2Bx + d^3C$$

or equivalently

$$dy^2 = x^3 + Ax^2 + Bx + C. \tag{10}$$

The impact of a quadratic twist on the singular fibers is well understood thanks to Tate's algorithm [24]. The fiber type stays the same if d vanishes to even order at the corresponding cusp on X. In case of odd vanishing order, the fiber types change in a canonical way unless the characteristic is three and there is wild ramification

(see e.g. [13]). For instance, fibers of type I_n are always interchanged with I_n^* in Kodaira's notation.

In the case of elliptic modular surfaces, we can use some crucial extra information. Namely, any (complex) elliptic modular surface is extremal: it has maximal Picard number $\rho(S) = h^{1,1}(S)$, but finite group of sections. By a theorem of Nori [17], these conditions (with j non-constant) imply the absence of singular fibers of type II, III, IV, I_0^*.

In consequence, on elliptic modular surfaces of different lifts of $\bar{\Gamma}$, the quadratic twisting can only occur at two kinds of points on $X(\Gamma)$:

- cusps underneath singular fibers of type $I_n, I_n^*(n > 0)$. Note that the local monodromy at these fibers is
$$T^n \quad \text{resp.} \quad -T^n.$$
- points such that d vanishes to even order.

Conversely, any such twist is again modular by [17]. Since it has the same modular curve X by construction, the projective images of the associated subgroups have to coincide. Since at twisting points of the second kind the fiber type does not change, the problem of detecting isomorphic elliptic surfaces is non-trivial; Stiller gave an example of this phenomenon in [23] related to the commutator subgroup of $SL_2(\mathbb{Z})$. There are no points of the second kind if the modular curve $X(\Gamma)$ is rational. The following two examples go back to section 5. Equations can be found in [13] for instance, but the cusps are normalised in a different manner than in section 5.

10.1. **Example:** $\Gamma_1(4)$**.** The elliptic modular surface for $\Gamma_1(4)$ is rational over $\mathbb{Q}$ with singular fibers of types I_1, I_4, I_1^*. Two of the twists are rational as well, while the twist with three non-reduced fibers is K3. In terms of Example 17, this modular surface corresponds to the congruence lift G_3. Recall that $S_3(G_3)$ has dimension one. To find the normalised cusp form, we use that its square is in $S_6(G_3) = S_6(\Gamma_1(4))$. The latter space is also one-dimensional and generated by $\eta(2\tau)^{12}$. Hence $S_3(G_3)$ is generated by $\eta(2\tau)^6$.

This K3 surface is also modular in another sense: its zeta function contains a factor corresponding to (a twist of) $\eta(4\tau)^6$, the unique weight 3 newform of level 16. We emphasise that the two cusp forms $\eta(2\tau)^6$ and $\eta(4\tau)^6$ have Fourier expansions in terms of different uniformisers, but with the same Fourier coefficients.

The modularity of the zeta function follows from a more general result by Livné [11]. In particular, this result applies to all singular K3 surfaces over $\mathbb{Q}$, i.e. with maximal Picard number $\rho = 20$. We will see more instances of this modularity in the next example, but first we shall point out a general fact in this context.

The above arithmetic relations with modular forms should not be seen as a surprise. In fact, Shioda showed in [22] that there is an analytic isomorphism

$$S_3(\Gamma) \cong H^{2,0}(S(\Gamma)) \tag{11}$$

between cusp forms of weight 3 with respect to Γ and holomorphic 2-forms on $S(\Gamma)$. In the congruence case, this isomorphism admits an arithmetic interpretation. Namely, $S(\Gamma)$ has a model over $\mathbb{Q}$. By Deligne [4], the Galois representation on the cohomology of $S(\Gamma)$ splits off two-dimensional subrepresentations. Here the traces of Frobenius correspond to eigenvalues of the Hecke operators on $S_3(\Gamma)$ as we have seen in the example above. In the noncongruence case, there is a

conjectural congruence relation due to Atkin–Swinnerton-Dyer (cf. [12] and the references therein).

10.2. **Example: $\Gamma_1(6)$.** We conclude this paper with a detailed analysis of the elliptic modular surface S for $\Gamma_1(6)$. We study the lifts of $\Gamma_1(6)$ and compute the corresponding cusp forms of weight 3. Then we compare with the zeta function of the corresponding twists of S.

A model of S over $\mathbb{Q}$ can be given as follows:

$$S: \quad y^2 = x(x^2 + (t^2 - 6t - 3)x + 16t).$$

Either six-torsion section $(4t, \pm 4t(t-1))$ generates the Mordell-Weil group of S:

$$\mathrm{MW}(S) = \{(4t, \pm 4t(t-1)), (4, \pm 4(t-1)), (0,0)\}.$$

The j-invariant of S is

$$j = \frac{(t-3)^3(t^3 - 9t^2 + 3t - 3)^3}{(t-9)(t-1)^3 t^2}.$$

One can describe the elliptic parameter t by

$$t = 9\eta(2\tau)^4\eta(3\tau)^8\eta(\tau)^{-8}\eta(6\tau)^{-4}.$$

The connection with the set-up in Example 18 is summarised in the following table:

cusp c	∞	$1/3$	$1/2$	0
width	1	2	3	6
$t(c)$	9	0	1	∞
stabilizer	T	AB^{-1}	B	AT

Thus S is a rational elliptic surface with singular fibers of types I_1, I_2, I_3, I_6. As explained, the different lifts of $\Gamma_1(6)$ from $\mathrm{PSL}_2(\mathbb{Z})$ to $\mathrm{SL}_2(\mathbb{Z})$ correspond to twists of S by certain $d \in \mathbb{Q}(t)$ as in (10). We collect this information in the next table. Six of the twists are K3 surfaces as indicated. The zeta function of each of them again contains a factor corresponding to some newform of weight three by [11]. The precise newform depends on the model of the K3 surface. By the classification in [20], very few Fourier coefficients suffice to determine the newform (see [20, Rem. 2.]). In the present situation, we achieved this by point counting at the first few good primes through Lefschetz' fixed point formula.

We express the resulting newforms in terms of some particular newforms (which are minimal in the sense of [20]) involving twists by the Legendre symbols $\chi_u = (u/p)$. Let

$$f_8 = \eta(\tau)^2\eta(2\tau)\eta(4\tau)\eta(8\tau)^2, \quad f_{12} = (\eta(2\tau)\eta(6\tau))^3$$

and let f_{24} denote the newform of level 24 from [20, Table 1] (given by a Hecke character for $\mathbb{Q}(\sqrt{-6})$ of ∞-type 2 and conductor $(2\sqrt{-6})$).

The full quadratic twist of S is not K3, but has $h^{2,0} = 2$ and Euler number $e = 36$. In terms of the Enriques-Kodaira classification of algebraic surfaces, it is honestly elliptic (Kodaira dimension one). We compute the decomposition of its

zeta function in terms of cusp forms g_1, g_2 below (see (12)).

d	fibres	lift of $\Gamma_1(6)$	level	$\dim S_3$	zeta	surface
1	$1\ ,2\ ,3\ ,6$	$\langle\ T,\ \ A,\ \ B\rangle$	6	0	–	rational
$t-9$	$1^*,2\ ,3\ ,6^*$	$\langle -T,\ \ A,\ \ B\rangle$	–	1	$f_{24}\otimes\chi_3$	K3
$t(t-9)$	$1^*,2^*,3\ ,6$	$\langle -T,-A,\ \ B\rangle$	–	1	$f_8\otimes\chi_3$	K3
$(t-1)(t-9)$	$1^*,2\ ,3^*,6$	$\langle -T,-A,-B\rangle$	6	1	f_{12}	K3
$t(t-1)(t-9)$	$1^*,2^*,3^*,6^*$	$\langle -T,\ \ A,-B\rangle$	12	2	g_1,g_2	$e=36$
t	$1\ ,2^*,3\ ,6^*$	$\langle\ T,-A,\ \ B\rangle$	12	1	f_{12}	K3
$(t-1)$	$1\ ,2\ ,3^*,6^*$	$\langle\ T,-A,-B\rangle$	–	1	$f_8\otimes\chi_{-1}$	K3
$t(t-1)$	$1\ ,2^*,3^*,6$	$\langle\ T,\ \ A,-B\rangle$	–	1	$f_{24}\otimes\chi_2$	K3

In order to compute the cusp forms in $S_3(\Gamma)$ for the lifts Γ, we shall again argue with extracting square roots, this time from $S_6(\Gamma) = S_6(\Gamma_1(6))$. In contrast to the case in 10.1 where the dimensions matched exactly, we have to take into account the following subtlety for square roots of $f \in S_6(\Gamma_1(6))$: For $\sqrt{f}$ to define a holomorphic function with respect to the lift Γ, we require f to vanish quadratically at all regular cusps of Γ and at all zeroes in the upper half plane. In the present situation, this criterion suffices to find all cusp forms.

We shall use the following modular forms of weight one for $\Gamma_1(6)$:

cusps (and widths)	$\infty(1)$	$\frac{1}{3}(2)$	$\frac{1}{2}(3)$	$0(6)$
weight one forms for $\Gamma_1(6)$	order of vanishing			
$a=\frac{\eta(z)\eta(6z)^6}{\eta(2z)^2\eta(3z)^3}=q-q^2+q^3+q^4+\cdots$	1	0	0	0
$b=\frac{\eta(2z)\eta(3z)^6}{\eta(z)^2\eta(6z)^3}=1+2q+4q^2+2q^3+\cdots$	0	1	0	0
$c=\frac{\eta(3z)\eta(2z)^6}{\eta(6z)^2\eta(z)^3}=1+3q+3q^2+3q^3+\cdots$	0	0	1	0
$d=\frac{\eta(6z)\eta(z)^6}{\eta(3z)^2\eta(2z)^3}=1-6q+12q^2-6q^3\cdots$	0	0	0	1

Note that there are relations $c = a + b, d = b - 8a$. It follows that any product of six of them defines a weight 6 form for $\Gamma_1(6)$ – and cusp forms include the product $g = abcd = (\eta(\tau)\eta(2\tau)\eta(3\tau)\eta(6\tau))^2$ which in fact generates $S_4(\Gamma_1(6))$. Looking at dimensions, it follows that these cusp forms generate $S_6(\Gamma_1(6))$. A basis could be chosen as ga^2, gab, gb^2.

Consider the six lifts that geometrically correspond to K3 surfaces. For each lift Γ, we will exhibit a cusp form of weight 6 for $\Gamma_1(6)$ whose square root gives a cusp form of weight 3 for Γ. As we have seen in Example 18, each lift has two regular cusps where extracting a square root requires quadratic vanishing of the weight 6 cusp form f. At the two irregular cusps, simple vanishing of f suffices. By inspection, these conditions determine the following normalised cusp forms of

weight 6 for $\Gamma_1(6)$ whose square roots yield cusp forms of weight 3 for the six lifts:

cusps (and widths)	$\infty(1)$	$\frac{1}{3}(2)$	$\frac{1}{2}(3)$	$0(6)$	
weight six forms for $\Gamma_1(6)$	order of vanishing				lift
$abc^2d^2 = \eta(z)^5\eta(2z)^5\eta(3z)\eta(6z)$	1	1	2	2	$\langle -T, -A, B\rangle$
$a^2b^2cd = \eta(z)\eta(2z)\eta(3z)^5\eta(6z)^5$	2	2	1	1	$\langle T, -A, -B\rangle$
$a^2bc^2d = \eta(2z)^6\eta(6z)^6$	2	1	2	1	$\langle T, -A, B\rangle$
$ab^2cd^2 = \eta(z)^6\eta(3z)^6$	1	2	1	2	$\langle -T, -A, -B\rangle$
$a^2bcd^2 = \eta(z)^9\eta(2z)^{-3}\eta(3z)^{-3}\eta(6z)^9$	2	1	1	2	$\langle T, A, -B\rangle$
$ab^2c^2d = \eta(z)^{-3}\eta(2z)^9\eta(3z)^9\eta(6z)^{-3}$	1	2	2	1	$\langle -T, A, B\rangle$

In the congruence cases, the zeta function of the elliptic modular surface thus indeed agrees with that of the corresponding generator of $S_3(\Gamma)$. In the non-congruence cases, one easily checks the Atkin–Swinnerton-Dyer relations for the square root of the corresponding weight six form generating $S_3(\Gamma)$ (which does not have integral Fourier coefficients) and the cusp form associated to S (which is the indicated twist of f_8 or f_{24}).

Finally we come to the lift $\Gamma = \langle -T, \quad A, -B\rangle$ where all cusps are irregular. Here $S_3(\Gamma)$ is two-dimensional, and any product of two cusp forms gives a form in $S_6(\Gamma_1(6))$.

Lemma 37. *For the lift* $\Gamma = \langle -T, \quad A, -B\rangle$, *we have with* $\sqrt{g} = \eta(\tau)\eta(2\tau)\eta(3\tau)\eta(6\tau)$

$$S_3(\Gamma) = \langle \sqrt{g}a, \sqrt{g}b\rangle.$$

Proof. Fix a basis h_1, h_2 of $S_3(\Gamma)$. A priori, we only have $h_1, h_2 \in \mathbb{C}[[q^{1/2}]]$, but since their product is in $S_6(\Gamma_1(6))$ and thus in $\mathbb{C}[[q]]$, we actually deduce that either $h_1, h_2 \in q^{1/2}\mathbb{C}[[q]]$ or $h_1, h_2 \in q\mathbb{C}[[q]]$. Under the latter alternative we would have a cusp form $h \in q^2\mathbb{C}[[q]] \cap S_3(\Gamma)$. Then h^2, which is in $S_6(\Gamma_1(6))$, would vanish to order 4 at ∞. In comparison, the cusp form in $S_6(\Gamma_1(6))$ with the highest vanishing order at ∞ is ga^2, but the vanishing order is only three, contradiction.

Under the first alternative, there is a cusp form $h \in q^{3/2}\mathbb{C}[[q]] \cap S_3(\Gamma)$. Along the same lines as above, one deduces that $h^2 = \lambda g a^2$ for some $\lambda \in \mathbb{C}$. This shows that $\sqrt{g}a \in S_3(\Gamma)$. We proceed by considering the product $\sqrt{g}ah_1 \in S_6(\Gamma_1(6))$. In terms of our basis, we write this product as $g\gamma$ for some quadratic form $\gamma(a, b)$. By assumption, we can also write $h_1 = \sqrt{g\delta}$ for some quadratic form $\delta(a, b)$. This gives an equality of modular forms $a\sqrt{\delta} = \gamma \in M_2(\Gamma_1(6))$. Upon squaring, we obtain the relation $a^2\delta = \gamma^2$ in $M_4(\Gamma_1(6))$. Since $M_4(\Gamma_1(6))$ has basis $a^4, a^3b, a^2b^2, ab^3, b^4$, spelling out the last relation shows that the quadratic form δ is in fact the square of a linear form in a, b. As the same argument applies to h_2, the lemma follows. □

Lemma 37 exhibits a basis of the vector space $S_3(\Gamma)$. Recall that the lift Γ is congruence. Hence the zeta function of the elliptic modular surface $S = S(\Gamma)$ encodes the Fourier coefficients of another basis g_1, g_2 of $S_3(\Gamma)$ which consists of Hecke eigenforms. We compute the relevant degree 4 factors $L_p(T)$ of the zeta function of S at the first few good primes with Lefschetz' fixed point formula (over $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$). We then read off the resulting Fourier coefficients a_p of g_1, g_2 (up to

conjugacy) from the real quadratic factors of $L_p(T)$:

p	$L_p(T)$	a_p
5	$T^4+18T^2+5^4$	$\pm 4\sqrt{2}$
7	$(T^2+6T+49)^2$	-6
11	$T^4+210T^2+11^4$	$\pm 4\sqrt{2}$
13	$(T^2-20T+13^2)^2$	20
17	$T^4+66T^2+17^4$	$\pm 16\sqrt{2}$

With some linear algebra on the vector space $S_3(\Gamma)$, one then verifies that (for the right sign choices between the Fourier coefficients of g_1 and g_2)

$$(g_1+g_2)/2=\sqrt{g}b,\quad (g_1-g_2)/(2\sqrt{2})=\sqrt{g}a. \tag{12}$$

Acknowledgement. We are indebted to Andreas Schweizer for pointing out a mistake in an earlier version of this paper. Our thanks go to the referee for several comments that helped improve the paper.

References

[1] W. Bosma, J. Cannon, C. Playoust: 'The Magma algebra system. I. The user language', J. Symbolic Comput. **24** (1997), 235–265.
[2] S.-P. Chan, M.-L. Lang, C.-H. Lim, S.-P. Tan: 'Special polygons for subgroups of the modular group and applications', Internat. J. Math. **4** (1993), no. 1, 11–34.
[3] Y. Chuman: 'Generators and relations of $\Gamma_0(N)$', J. Math. Kyoto Univ. **13** (1973), 381–390.
[4] P. Deligne: 'Formes modulaires et représentations ℓ-adiques,' Sém. Bourbaki 1968/69, no. 355 (Lect. Notes in Math. **179**), Springer-Verlag (1971), 139–172.
[5] A. Dooms, E. Jespers, A. Konovalov, H. Verrill. *Congruence — Congruence subgroups of* $SL_2(\mathbb{Z})$, GAP package, in development.
[6] H. Frasch: 'Die Erzeugenden der Hauptkongruenzgruppen für Primzahlstufen', Math. Ann. **108** (1933), no. 1, 229–252.
[7] GAP - Groups, Algorithms, Programming - a System for Computational Discrete Algebra, http://www.gap-system.org
[8] R. S. Kulkarni: 'An arithmetic-geometric method in the study of the subgroups of the modular group', Amer. J. Math. **113** (1991), 1053–1133.
[9] M.-L. Lang, C.-H. Lim, S.-P. Tan: 'An algorithm for determining if a subgroup of the modular group is congruence', J. London Math. Soc. (2) **51** (1995), no. 3, 491–502.
[10] H. Larcher: 'The cusp amplitudes of the congruence subgroups of the classical modular group', Illinois J. Math. **26** (1982), no. 1, 164–172.
[11] R. Livné: 'Motivic Orthogonal Two-dimensional Representations of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$', Israel J. of Math. **92** (1995), 149–156.
[12] L. Long: 'Finite index subgroups of the modular group and their modular forms', Modular forms and string duality, 83–102, Fields Inst. Commun. **54**, Amer. Math. Soc., Providence, RI, 2008.
[13] R. Miranda, U. Persson: 'On Extremal Rational Elliptic Surfaces', Math. Z. **193** (1986), 537–558.
[14] T. Miyake: 'Modular Forms', Springer 1989.
[15] M. Newman: 'Normal congruence subgroups of the modular group', Amer. J. Math. **85** (1963), 419–427.
[16] M. Newman, J. R. Smart: 'Note on a subgroup of the modular group', Proc. Amer. Math. Soc. **14** (1963), 102–104.
[17] M. Nori: 'On certain elliptic surfaces with maximal Picard number', Topology **24** (1985), no. 2, 175–186
[18] PARI/GP, version `2.3.4`, Bordeaux, 2008, http://pari.math.u-bordeaux.fr/.
[19] H. Rademacher: 'Über die Erzeugenden von Kongruenzuntergruppen der Modulgruppe', Abh. Math. Sem. Univ. Hamburg **7** (1929), 134–148.
[20] M. Schütt: 'CM newforms with rational coefficients', Ramanujan J. **19** (2009), 187–205.

[21] G. Shimura: 'Introduction to the Arithmetic Theory of Automorphic Functions', Princeton University Press 1971.
[22] T. Shioda: 'On elliptic modular surfaces', J. Math. Soc. Japan **24** (1972), 20–59.
[23] P. Stiller: 'On the classification of elliptic surfaces with $q = 1$', Manuscripta Math. **60** (1988), 299–321.
[24] Tate, J.: *Algorithm for determining the type of a singular fibre in an elliptic pencil*, in: *Modular functions of one variable IV* (Antwerpen 1972), Lect. Notes in Math. **476** (1975), 33–52.
[25] K. Wohlfahrt: 'An extension of F. Klein's level concept', Illinois J. Math. **8** (1964), 529–535.

(Ian Kiming) Department of Mathematical Sciences, University of Copenhagen, Universitetsparken 5, 2100 Copenhagen Ø, Denmark
E-mail address: kiming@math.ku.dk

(Matthias Schütt) Institut für Algebraische Geometrie, Leibniz Universität Hannover, Welfengarten 1, 30167 Hannover, Germany
E-mail address: schuett@math.uni-hannover.de

(Helena A. Verrill) Department of Mathematics, Louisiana State University, Baton Rouge, Louisiana 70803-4918, USA
E-mail address: verrill@math.lsu.edu